Вопросы к экзамену по дисциплине «Защита информации»

1. Основы информационной безопасности. Основные составляющие информационной безопасности.

2. Основы информационной безопасности. Объекты защиты. Категории и носители информации.

3. Классификация средств защиты информации.

4. Шифрование. Основные термины и определения. Требования, предъявляемые к криптосистемам.

5. Классификация криптографических систем.

6. Шифры замены. Основы. Класификация.

7. Шифры однозначной замены. Шифр Цезаря. Атбаш. Лозунговый шифр.

8. Шифры однозначной замены. Полибианский квадрат. Шифрующая система Трисемуса.

9. Полиграммные шифры

10. Омофонические шифры

11. Полиалфавитные шифры

12. Нерегулярные шифры

13. Шифры перестановки. Основы. Классификация.

14. Шифры одинарной перестановки. Шифр простой одинарной перестановки. Шифр блочной одинарной перестановки. Шифр табличной маршрутной перестановки.

15. Шифры одинарной перестановки. Шифр вертикальной перестановки. Шифр «Перекресток». Шифр с использованием треугольника

16. Шифры одинарной перестановки. Шифр «Поворотная решетка». Магические квадраты.

17. Шифры множественной перестановки.

18. Шифрование с открытым ключом. Основы. Типы односторонних преобразований.

19. Алгоритм RSA.

20. Алгоритм на основе задачи об укладке ранца.

21. Вероятностное шифрование.

22. Алгоритм шифрования Эль-Гамаля.

23. Комбинированные шифры. ADFGX и ADFGVX.

24. Комбинированные шифры. Основы блочного комбинированного шифрования.

25. DES. Схема шифрования блока.

26. DES. Режимы - сцепление блоков шифра; обратная связь по шифртексту; обратная связь по выходу. Тройной DES.

27. ГОСТ 28147-89.

28. Шифры гаммирования. Основы. Сложение по модулю 2.

29. Хеш-функции. Применение шифрования для получения хеш-образа.

30. MD5.

31. Стенография. Классификация классических методов.

32. Компьютерная стенография. Классификация методов.